REMARKS

Applicant's counsel thanks the Examiner for the careful consideration given the application. Applicant's counsel thanks the Examiner for the courteous telephone interview conducted on May 11, 2006 in which applicant's counsel John Harris, applicant's technical consultant Sumiko Mori, Examiner Truong, and SPE David Wiley participated. During the interview, applicant's counsel discussed U.S. Patent Numbers 5,979,754 and 5,850,753 and explained how the claims as now amended defined over these references. The Examiners after the discussion stated that they would allow the case with the claims as they are now amended.

The present application contains claims 1 and 4 to 47.

Claims

Claim 1 has been amended to clarify the separation of key administration and door administration by reciting module for managing the one or more keys and assigning a key to the key owner independently from the access privilege for each door. Claim 1 has been amended to clarify that the door is operated based on the access privilege of the key user when the identified user key is a key administered by the key administering system, and the key user is an individual authorized to one or more doors by the door administering system and having access authorization to the door.

Claim 20 has been amended to add changes corresponding to those of claim 1.

The amendments to claims 1 and 20 are fully supported by the application as originally filed, for example, on page 16, lines 4 to 5 and page 16, line 26 to page 17, line 1 and in Figures 1 and 3. "module for managing the one or more keys" is reasonably inferred from the originally filed application, and can be read by a person skilled in the art.

Claim 10 has been amended to replace "the user's key" with --the user key--, and to replace "the user of the key" with --the key user--.

No new matter has been introduced by way of the amendments to the claims.

Claim rejections-35 U.S.C 103(a)

1) The Examiner rejected claims 1, 4-5, 8, 10, 13, 15-18, 20, 28-36, 39-44 and 46 as being unpatentable over Martin et al. (US 5,979,754), hereinafter referred to as Martin, in view of Varma (U.S. 5,850,753).

Applicant respectfully requests reconsideration and withdrawal of the rejections.

Independent Claim 1

According to independent claim 1, a door administering system includes a module for managing access privilege of one or more individual for each door, and a key administering system includes a module for managing one or more keys independently from the access privilege of the one or more individual for each door. When a key user presents a user key, a door control/lock assembly operates on a door based on the access privilege of the key user if the user key is a key administered by the key administering system, and the key user is an individual authorized to any of the one or more doors by the door administering system to the door and having access authorization to the door.

According to the present invention, the key administration is separated from the door administration. Thus, the door control/lock assembly operates a door in cooperation with the key administration and door administration.

Separating the administrative functions of key administration and door administration from each other ensures that each function can be administered by different individuals who do not necessarily have access to the other administrative function. This allows key information in the key administering system to be changed without access to information in the door administering system. Similarly, this allows a new key to be registered with the key administering system without access to the information in the door administering system. Accordingly, the registered key can be quickly and easily updated (replaced or cancelled), and a new key can be quickly and easily stored in the key administering system.

Further, a single key, assigned at the key administering system, may be used to unlock many doors as authorized by the door administering system. Changing of the key at the key administering system affects the relationship between that key and the doors to which access has been granted. Similarly, a single door may have

authorized access by many separate keys, each registered in its own key administering system.

To illustrate how the system of claim1 operates under the separation between the key administration and the door administration, Applicant attaches an example for the Examiner's review [Example 1].

As discussed on the Applicant's correspondence submitted on January 6, 2006, the system of Martin contains no provision for a user to change his identity card once he has been given permission to operate a particular door.

On page 4 of the Office Action, the Examiner stated:

> -- Martin discloses "guest's credit card is equal to "unique key" for the assigned room" -- [Emphasis added]

Martin's credit card provides access authorization to a card holder for the assigned room. By contrast, the key of claim 1 is uniquely assigned to a key owner, and is not a key uniquely assigned for the assigned room.

On page 4 of the Office Acton, the Examiner stated:

> -- Martin does not explicitly teach a key administering system for administering one or more keys separately from the administration of the access to the door, each key being uniquely assigned to a key owner ...--

On page 5 of the Office Acton, the Examiner then stated:

> -- However, Varma discloses "a card reader" which is equivalent to "a key administering system" can be updated by itself with "a new access code" which is equivalent to "a key." When the guest departures, the hotel cleaning staff changes the guest access code from card reader. The computer at front desk is physically separated with card reader and updated the new access code, see (Varma: column 1, lines 31-59)
>
> Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Varma's ideas of the hotel staff changes access code for card reader with Martin's system in order to provide separated operation system those either can update guest access code, see (Varma: column 1, lines 31-59)--

Applicant respectfully disagrees with the Examiner.

Col. 1, lines 19-20 of Varma states:

> -- A magnetic card reader is mounted directly to the door of a hotel room--

Col. 1, lines 26-27 of Varma states:

> -- A guest will normally receive a card bearing an access code unique to his room. The guest's code is typically assigned by a computer at the front desk of the hotel upon registration. – [Emphasis added]

Col. 1, lines 32-35 of Varma states:

> -- After a guest's departure, hotel cleaning staff trigger the card reader to change the guest access code, and the card reader then updates the access code according to a predetermined algorithm. The computer at the front desk of the hotel normally stores all guest access codes and uses the same algorithm as the card readers to update guest access codes. --.

Varma's card stores an access code (α). Varma's card reader is mounted on a specific door and stores an access code (β) to open the door. Varma's card reader reads the access code (α) from the card presented by the card holder and opens the door based on the access code (α) read from the card and its own access code (β). To prevent the card holder from accessing the door, Varma's card reader changes its own access code (β). In other words, Varma's card reader administers door access. Varma's card reader manages its own access code (β) to allow the card holder to access the door or remove the access authentication to the card holder for that door by changing its own access code (β).

The Examiner considered that the access code of Varma is a key assigned to the card holder. However, Varma's card reader does not assign a key (access code α or β) to the card holder. Therefore, the access code (α, β) of Varma is not a key of claim 1, because in claim 1, the key is uniquely assigned to a key owner by the key administering system. The access code of Varma provides access authentication to the card holder for the door, and thus is a code to identify the door.

Varma merely discloses a computer physically separately from the card reader. There is no suggestion or teaching in Varma that the key (access code) administration is provided independently from the door administration.

Accordingly, Varma does not add any teaching to Martin to render claim 1 unpatentable.

Independent claim 20

Claim 20 is directed to a method of implementing door access control and key management via a communications network. Claim 20 corresponds to claim 1, and recites a door server, a key server and a door control/lock assembly. At the door server, access to one or more doors is administered, which includes: managing access privilege of one or more individuals for each door and assigning access authorization to each individual for the door. At the key server, one or more keys are administered separately from the administration of the access to the door, which includes: managing the keys and assigning a key to a key owner independently from the access privilege of the one or more individual for each door. At the door control/lock assembly, a user key presented by a key user is identified. The identified user key is compared to the keys of the key owners. A door is operated based on the access privilege of the key user by verifying that the identified user key is a key administered by the key server and the key user is an individual authorized to any one or more doors by the door server and having access authorization to the door.

With respect to the rejection of claim 20, the Examiner stated:

> -- Varma discloses the communication between "a card reader" which is equivalent to "a key administering system" and "the computer at front desk" which is equivalent to "the administration of the access to the door" to operate for door opening; wherein the computer at front desk assigns the guest's assess code used for authorization to operate the door, see (Varma: column 1, lines 31-59). -- (on page 7 of the Office Action)

As discussed above, Varma's card reader manages door access. Varma's card reader cannot assign the access code (α, β) to a card holder, and cannot manage the access code (α, β) independently from the access privilege of the card holder for that door. Thus, Varma's card reader is not a key server of claim 20.

Dependent claims

Claims depending on claims 1 and 20 contain further features.

Claim 4 depends on claim 1, and recites that the door control/lock assembly carries out the authorization process when the communication between the door control/lock assembly and the door and key administering systems is interrupted.

With respect to the rejection of claim 4, the Examiner stated:

> -- Martin discloses after the guest runs the "proper credit card" is "room key" through "his/her guest room card reader" which is equal to "door control/lock assembly", the "computer" which is equal to "door administering system" recognizes and accepts that the [sic] guest card as an approved key, then a signal is transmitted to the door transceiver causing the lock to open to an approved card.: column 4, lines 21-45, 62-67; column 7, lines 30-44) -- (on page 7 of the Office Action)

Thus, according to the Examiner's statement, the guest room card reader of Martin is a door control/lock assembly of claim 4, while the computer of Martin is the door administering system of claim 4 and recognizes and accepts the guest card as an approved key.

However, there is no disclosure or suggestion in Martin that the guest card reader (door control/lock assembly) carries out the authorization process when the communication between the computer (door administering system) and the guest room card reader (door control/lock assembly) is interrupted, as recited in claim 4. There is no disclosure or suggestion in Varma that Varma's card reader carries out the authorization process when the communication between Varma's computer and Varma's card reader is interrupted, as recited in claim 4. Thereof, even if combining Martin and Varma, the combination cannot achieve the subject matter defined by claim 4.

Claim 10 depends on claim 1, and recites that the door control/lock assembly includes an identification device, a lock adapted to be operated in response to the authorization from the door and key administering systems, and an embedded controller for controlling the operation of the identification device and the lock, and the authorization process.

With respect to claim 10, the Examiner stated:

> -- Martin discloses if the "computer" which is equivalent to "door/key administering system" that is located at a central control center recognizes and accepts that guest card as an approved card, then the computer generates a signal which is sent to door transceiver causing the lock to open to an "approved card" which is equivalent to "room key...-- (on page 9 of the Office Action)

As acknowledged by the Examiner on page 4 of the Office Action, Martin fails to suggest a key administering system for administering one or more keys separately from the door administration. Varma's card reader is mounted on a specific door. Varma's card reader operates a door based on its access code (β), and does not operate the door based on its access code (β) and door authorization information from any other computers. Thus, even if combining Marin and Varma, the combination cannot achieve the subject matter defined by claim 10.

Claim 15 depends on claim 10, and contains features similar to claim 4. The above discussion to the rejection of claim 4 is applied to the rejection of claim 15.

Claim 28 depends on claim 1, and recites that the key owner of a key is capable of changing the key of that key owner at the key database.

With respect to the rejections of claim 28, the Examiner stated:

> -- Martin-Varma discloses the invention substantially as disclosed in claim 1, further teaches wherein the key owner of a key is capable of changing the key of that key owner at the key database ... Varma discloses when the guest departures, the hotel cleaning staff changes the guest access code from card reader, then the computer updates the new access code to provide to next guest.--

In Varma, the hotel cleaning staff changes the access ~~cord~~code (β) stored in the card reader. However, the hotel cleaning staff is not a "key owner" of a "key", since the access ~~cord~~code (α, β) to be changed by the hotel cleaning staff is not uniquely assigned to the hotel cleaning staff. By contrast, in claim 1, a key is uniquely assigned to a key owner, and in claim 28, that key owner is capable of changing its key. Furthermore, as discussed above, the access code (α, β) of Varma is not a key of claim 1.

Claims 30 and 31

Claim 30 depends on claim 1, and claim 31 depends on claim 31.

With respect to the rejections of claims 30-31, the Examiner stated:

> -- Martin discloses a "the computer" which represented of "door administering system" which stores the identity of all doors and rooms requiring control in a given facility, and identification of all individuals authorized to have entry to all or specific rooms of the facility and can associate a specific entry card with each room and each authorized person -- [Emphasis added] (on page 12 of the Office Action)

Claims 1, 30 and 31 do not recite that the door administering system associates any key with each room and each authorized person. According to claims 1, 30 and 31, the door administering system administers access to one or more doors, and manages access privilege of one or more individuals for each door, while the key administering system associates a specific key with each specific key owner.

Accordingly, even if combining Martin and Varma, the combination cannot render claims 1 and 20 and their dependent claims 4 to 19 and 21 to 47 unpatentable.

2) The Examiner rejected claim 9 as being unpatentable over Martin and Varma in view of Flick (U.S. 6,130,606).

Claim 9 depends on claim 1, and recites that the communication and authorization process between the door and key administering systems and the door control/lock assembly are carried out in a form of encrypted signals or messages.

By contrast, Flick merely discloses encryption. Flick discloses a vehicle security system including a controller having a remote transmitter verification means for generating a signal based upon a number of coded remote transmitters 50 capable of switching the controller from the armed mode to the disarmed mode (col. 5, lines 4-8). Flick's system is irrelevant to the present invention.

Further, as discussed above, Martin and Varma fail to suggest the subject matter defined by claim 1. Flick does not add any teaching to Martin and Varma to render claim 9 unpatentable.

3) The Examiner rejected claim 14 and 45 as being unpatentable over Martin and Varma in view of Dunhame et al. (U.S. 5,541,585), hereinafter referred to as Dunhame.

Claims 14 and 45 depend on claim 1, and recite an activity light.

The Examiner stated:

> --Dunhame discloses a security system for controlling building access that includes door open sensor, speaker and microphone, "dim light" which is equivalent to "activity light" and camera--

Dunhame discloses a security system having a dim light 22. The dim light 22 is mounted to door frame 12 and provides a low level of light to the door opening (col. 5, lines 16-17).

It is respectfully submitted that an activity light is an LED (light-emitting diode) that shines when a piece of hardware is working, communicating with the network, and transmitting data (www.watchguard.com/glossary/a.asp). The activity light of claim 14 is different from the dim light 22 of Dunhame.

Further, as discussed above, Martin and Varma fail to suggest the subject matter defined by claim 1. Dunhame does not add any teaching to Martin and Varma to render claims 14 and 45 unpatentable.

4) The Examiner rejected claim 25 as being unpatentable over Varma in view of Bengtsson et al. (U.S. 6,356,942), hereinafter referred to as Bengtsson.

Claim 25 recites a plurality of door access control and key management systems, each of which is the system of claim 1, and a Meta server. The Meta server is communicatively and operatively connected to each of the door access control and key management systems (of claim 1), via the commutations network, wherein the Meta server contains the address of each separate door administering system (of claim 1) and key administering system (of claim 1).

The door administering system(s) and the key administering system(s) and the Meta server work together to communicate a specific key, associated with a specific person by the key administering system, to one or many specific doors to which the specific person has been given access by one or many door administering systems.

If the specific person changes their key (access card) by using their key administering system (or if an authorized key administrator does it for them) then the changed key (access card) information is communicated to all of the doors to which the specific person has been given access by means of the key administering system and door administering systems working together with the help of the Meta server.

To illustrate how the system of claim 25 operates, Applicant encloses an example for the Examiner's review [Example 2].

The Examiner stated:

> -- Bengtsson discloses "a server" which is equivalent to "a meter server" being adapted to service as an address reference for communication between peripheral devices: (abstract, lines figure 1D; column 9, lines 1-67; column 10, lines 1-67)
>
> Thus, it would have obvious to a person of ordinary skill in the art at the time the invention was made to combine Bengtsson's ideas of using a server being serviced as an address reference with Varma's system in order to speed up communication process – (on page 15 of the Office Action)

According to the above Examiner's statement, Bengtsson's server is to "speed up" the communications process. By contrast, the meta server of claim 25 acts as an address reference so that door administering systems can locate the key administering system that holds the specific key information associated with a specific individual from among a potentially large number of key administering systems on a communication network. Bengtsson does not disclose or suggest this feature.

Claim 25 depend on claim 1. As discussed above, Varma fail to suggest a key administering system as recited in claim 1. Even if Bengtsson discloses a server, Bengtsson does not add any teaching to Varma to render claim 25 unpatentable.

5) The Examiner rejected claims 11-12 and 21-22 as being unpatentable over Martin and Varma in view of Yulkowski (U.S. 6,049,287).

Claim 11 depends on claim 1, and recites that each key owner has one or more keys for the door, and the door control/lock assembly includes two or more identification devices. Claim 12 depends on claim 11.

Claim 21 depends on claim 20, and recites storing two or more different unique key signatures for the user whereby all of the different key signatures are required to gain access to the door. Claim 22 depends on claim 21.

The Examiner stated:

> -- Yulkowski discloses a controller may be an access control device has both a "keypad and card reader" those are equivalent to "identification devices".--

The key pad 68 of Yulkowski allows the input of an identification code to the controller 66 to allow the door to unlock or lock. The card reader 70 of Yulkowski may be used to inert or slide a card therethrough to unlock or lock the door (col. 4, lines 66-64). Yulkowski merely discloses that a card and an identification code are required to gain access within an opening (col. 4, lines 65-67). The key pad and card reader of Yulkowski does not communicate with a door administering system (or a door server) and a key administering system (or a key server).

Further, as discussed above, Martin and Varma fail to suggest the subject matter defined by claims 1 and 20. Even if Yulkowski discloses a keypad and a card reader, Yulkowski does not add any teaching to Martin and Varma to render claims 11-12 and 21-22 unpatentable.

6) The Examiner rejected claims 6-7, 19 and 23 are rejected as being unpatentable over Martin and Varma in view of Kalajan (U.S. 6,006,258).

Claims 6-7 and 19 depend on claim 1. Claim 23 depends on claim 20.

Kalajan is directed to a method and system for delivering a message unit to a destination network resource. Kalajan merely discloses protocols, and is not relevant to door access and key management.

Further, as discussed above, Martin and Varma fail to suggest the subject matter defined by claims 1 and 20. Even if Kalajan discloses an Internet Protocol communication, Kalajan does not add any teaching to Martin and Varma to render claims 6-7, 19 and 23 unpatentable.

7) The Examiner rejected claim 26 as being unpatentable over Varma and Bengtsson in view of Kalajan.

Claim 26 depends on claim 25. Claim 25 depends on claim 1. As discussed above, Varma fail to suggest a key administering system as recited in claim1. As discussed above, Bengtsson's server is not a Meta server of claim 25. Even if Kalajan discloses a transport protocol, Kalajan does not add any teaching to Varma and Bengtsson to render claim 26 unpatentable.

8) The Examiner rejected claim 27 as being unpatentable over Varma and Bengtsson in view of Paxhia et al. (US Patent Application Publication 2002/0052935), hereinafter referred to as Paxhia.

Claim 27 depends on claim 25. Claim 25 depends on claim 1. Varma fail to suggest a key administering system as recited in claim1. Bengtsson's server is not a Meta server of claim 25 as described above. Even if Paxhia discloses Netscape, Paxhia does not add any teaching to Varma and Bengtsson to render claim 27 unpatentable.

9) The Examiner rejected claim 37-38 as being unpatentable over Martin and Varma in view of Saliga (US Patent No. 5,397, 884).

Claims 37-38 depend on claim 1. Varma fail to suggest a key administering system as recited in claim1. Even if Saliga discloses setting a predetermined authorization time period, Saliga does not add any teaching to Martin and Varma to render claims 37-38 unpatentable.

In view of the above amendments and remarks and having dealt with all the objections raised by the Examiner, reconsideration and allowance of the application is courteously requested.

If there are any further fees required by this communication, please charge such fees to our Deposit Account No. 16-0820, Order No. 34118.

Respectfully Submitted,

PEARNE & GORDON LLP

By _____
John P. Murtaugh, Reg. No. 34226

1801 East 9th Street
Suite 1200
Cleveland, Ohio 44114-3108
(216) 579-1700

Date: 5-30-06